MATERIAL CONTROL STUDY: A DIRECTED GRAPH AND FAULT-TREE PROCEDURE FOR ADVERSARY EVENT SET GENERATION†

H.E. Lambert*, J.J. Lim**
and F.M. Gilman**

*TERA Corp., Berkeley, CA 94704
**Lawrence Livermore Laboratory,
Livermore, CA 94550

ABSTRACT

Lawrence Livermore Laboratory is developing an assessment procedure to evaluate the effectiveness of a potential nuclear facility licensee's material control (MC) system. The purpose of an MC system is to prevent the theft of special nuclear material such as plutonium and highly enriched uranium. The key in the assessment procedure is the generation and analysis of the adversary event sets by a directed graph and fault-tree methodology. The methodology is described step-by-step and its application illustrated by an example.

1. INTRODUCTION

The Lawrence Livermore Laboratory is conducting a Material Control and Accounting Study for the Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research. As part of their duties, the NRC is responsible for the licensing of new nuclear facilities. Since the safeguarding of nuclear materials has become increasingly important in recent years, the NRC must be able to systematically evaluate the material control systems of proposed nuclear facilities and to guarantee their effectiveness to the public. Each facility has a material control system to protect against the theft of special

†This report was prepared for the U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research under research order No. 66-77-012 and under the auspices of the U.S. DOE, Contract No. W-7405-ENG-48.

nuclear material, SNM, such as plutonium and uranium 235. In the three year-old study the Laboratory has been developing an assessment procedure to evaluate the effectiveness of a potential nuclear licensee's material control system.[1]

The assessment procedure, shown in the block diagram in Figure 1, needs two types of data: license applicant information and the NRC/LLL data base. Applicant data include the plan of the facility physical plant, operational procedures, descriptions of special nuclear material processing, and the details of the material control and accounting system. The NRC/LLL data base will contain the mathematical models (such as models of the performance of the SNM detection monitors) necessary to evaluate an applicant's submittal.

The first step in the assessment procedure is to identify targets within the facility that contain theft-attractive SNM. The second step is to determine the adversary actions and conditions of the material control system that could allow successful diversion of special nuclear material, that is, generate the adversary event sets. Simulation of the events is required for those adversary event sets where timeliness and ordering of events is important for successful diversion. The qualitative and quantitative analysis of the event sets and the simulation results allow the effectiveness of the material control system to be determined.

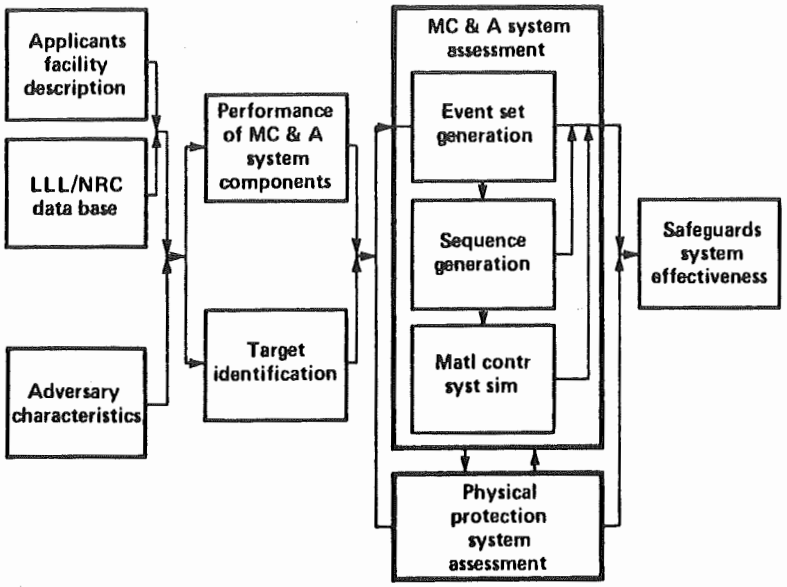

Figure 1. The LLL Assessment Procedure

2.0 ADVERSARY EVENT SET GENERATION PROCEDURE

The key in the LLL assessment procedure for evaluating the effectiveness of a material control system is the generation and analysis of adversary event sets. We have developed a procedure based on a directed graph (digraph) and fault-tree methodology by which the event sets can be generated and analyzed. This methodology has been used by Lapp and Powers[2] to assess the safety of chemical processing systems. As described by Lambert and Lim[3], this methodology was extended to model intentional diversionary or malevolent acts by an adversary so that these acts appear in the event sets.

The procedure for the generation and analysis of the event sets is next described, in detail, as delineated by the block diagram in Figure 2.

2.1 General System Schematic

The first step in the procedure (Figure 2) is the formulation of a general schematic for system modeling. Information from piping and instrumentation diagrams, the physical plant layout, and material control related procedures is used to formulate the schematic for

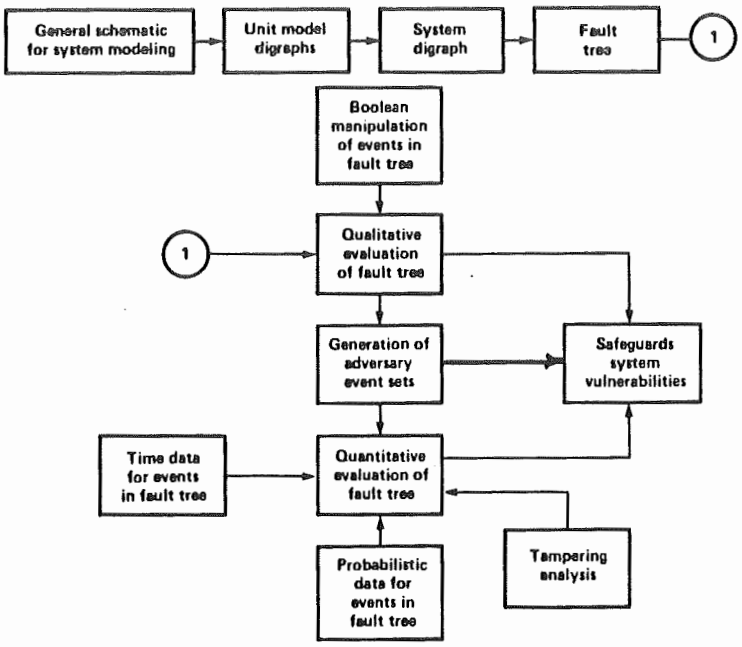

Figure 2. Procedure For Generation and Analysis of Adversary Event Sets

system modeling. The general schematic delineates the unit model digraphs needed to model the system and the overall system interactions. The unit models include models of adversary movement in the facility, monitors, process equipment, and procedures.

2.2 Unit Model Digraphs

In step 2 (Figure 2), unit model digraphs, the basic building blocks of the procedure, are generated. Digraphs are functional cause-and-effect network models that describe the relationship between various system variables and the conditions that are necessary for these relationships to exist.[2,3] In addition, digraphs can show events such as adversary actions that may nullify or change the relationships between variables. Digraphs are useful since they are multivalued network models and they can readily model the dynamics of the relationships between variables. The advantage of generating unit model digraphs is that a separate analysis can be performed on system components without performing an entire system analysis. These unit models are analogous to mini-fault trees described by Fussell, et al[4] and decision tables described by Salem, et al.[5]

2.3 System Digraph

The third step in Figure 2 is the generation of the system digraph, which is constructed from the unit model digraphs for a selected top event variable (the top event is the event being modeled). The system digraph is obtained by deductively following the information flow given in the general system schematic. The material control system is modeled as a control system designed to counter the actions of the adversary. The potential ways the material control system may respond to prevent special nuclear material theft are modeled in terms of "adversary cancellation loops" of the system digraph. These loops are similar in concept to the negative feedback and negative feedforward control loops designed to cancel disturbances in process variables.

2.4 System-Fault Tree

In the fourth step (Figure 2), the system-fault tree is generated from the system digraph via a synthesis algorithm. The top event in the fault tree corresponds to a disturbance in the top event variable of the system digraph. The top event variable for the material control study is M_{DIV}, defined by

$$M_{DIV} = \begin{cases} +1 \text{ if sucessful diversion of} \\ \text{special nuclear material occurs} \\ 0 \text{ otherwise} \end{cases}$$

A zero value for a variable on the system digraph corresponds to a true or expected value. Any other value, hence, corresponds to a deviation or disturbance. The top event in the system fault tree for the material control study is M_{DIV}= +1. All loops in the system digraph that model the corrective actions of the material control system must fail for a disturbance in the top event variable to exist.

For successful diversion of SNM to occur, all adversary cancellation loops must fail. These loops fail as the result of:

- random monitor failure
- inadequate monitor measurement sensitivity
- human error, including slow guard response
- adversary activity, including equipment tampering and collusion

The synthesis algorithm creates an AND logic gate in the fault tree each time a cancellation loop in the system digraph fails.

Once generated, the fault tree can be evaluated qualitatively and quantitatively to assess the vulnerabilities of the safeguard system.

2.5 Qualitative Analysis

The qualitative analysis of the fault tree provides much valuable information without using numerical data. It includes performing Boolean manipulations of the basic events, generating the adversary event sets, structurally ranking the basic events, determining the collusion requirements, and evaluating the effect of power loss on the material control system.

A structural ranking of the basic events in the event sets helps to identify important basic events for further analysis. This type of ranking is a function of the number of event sets in which a basic event appears in and the relative length of those event sets.

Common cause analysis is used to determine the collusion requirements (the number and identity of plant personnel) and the effects of power loss of key components of the material control system for successful special nuclear material theft. In addition, a vital location analysis can be performed to determine the locations which must be visited for successful tampering.

The computer codes Fault-Tree Analysis Program (FTAP)[6] and the Set Equation Transformation System (SETS)[7], designed to generate and handle numerous, high-ordered minimal cut sets, are used to perform the qualitative analysis.

2.6 Quantitative Analysis

To further identify the weaknesses of the material control system, a quantitative analysis is performed. This analysis assesses the impact of material control system components with various failure rates and detection probabilities, the effect of maintenance policies, and the ease with which component tampering can occur. The IMPORTANCE computer code[8] is used to perform the quantitative assessment.

Inputs required for the quantitative analysis are a listing of the event sets, probability data for the basic events, and the assumption of statistical independence of the basic events.

The probability of successful theft of special nuclear material can be calculated for four specific cases:

(1) No material control system tampering, no alarm signal generated.

(2) No material control system tampering, slow safeguards response.

(3) Material control system tampering, no alarm signal generated.

(4) Material control system tampering, slow safeguards response.

A sensitivity analysis of the probability of successful theft for the above cases as a function of the amount of special nuclear material stolen is also done. Quantities of SNM investigated are 0.5 g, 200 g, and 5 kg. The maximum expected performance of the material control system occurs when there is no system tampering. However, clever adversaries may tamper with the material control system to render it ineffective. In the tampering analysis, the following adversary attributes and material control system characteristics are considered:

- Type of tools and resources required for tampering
- Accessibility of components to potential adversaries
- Monitoring of equipment for tampering

- Availability of tools and resources required for tampering
- Personnel required for tampering

The probability of successful tampering is then a function of the probability that each of the above can occur with either no or slow material control system response.

3. DEMONSTRATION OF THE EVENT SET GENERATION PROCEDURE

The event set generation and analysis procedure has been applied in the assessment of the material control system[9] in a prototype nuclear facility, the Test Bed.[10]

3.1 Test Bed Assessment

The Test Bed is based upon the plutonium nitrate storage area of the Allied-General Nuclear Services, AGNS, facility in Barnwell, S.C., but with substantial modifications. These modifications are added to further develop and test the assessment procedure and are not criticisms or "fixes" to the AGNS current design. The modifications include the addition of check valves, limit switches on valves, a computer controlled access system, computerized material control and accounting and procedure monitoring logic, and other safeguards components.

The general form of the system digraph for the Test Bed is shown in Figure 3. The arrows represent information flow with regard to (1) movement of special nuclear material and people, and (2) the material control system response which acts to prevent the theft of special nuclear material. The initial conditions for the Test Bed assessment are shown on the left of Figure 3.

The fault tree generated from the system digraph by the synthesis algorithm contained 125 gate events and 113 basic events. The qualitative analysis of the fault tree generated 814,042 event sets for the case of no safeguards response. These adversary event sets ranged in length from 18 basic events to 28 basic events. These event sets were very descriptive and contained all the adversary acts necessary for successful diversion, including the route for adversary movement in and out of the facility.

The collusion analysis established that successful diversion can occur only if three particular plant personnel are in collusion or if two persons are in collusion when random failures occur.

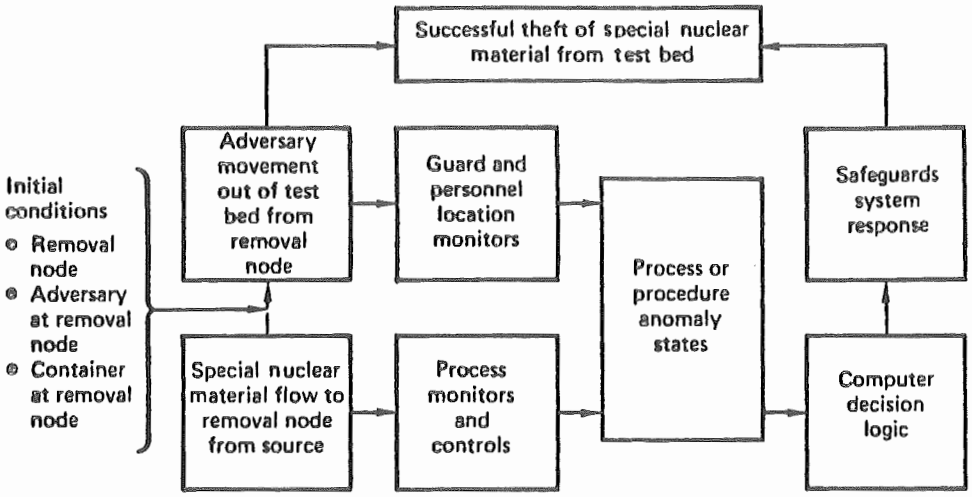

Figure 3. General Form of System Digraph for Test Bed

The IMPORTANCE computer code[8] determined the probability of each basic event contributing to the probability of successful diversion. The ranking of these basic events determined the following vulnerable points in the Test Bed:

computer hardware and software

remote control panel

crash door alarms

maintenance policies

Although the Test Bed is a facility with an automated and sophisticated material control system, the assessment has found several basic weaknesses. A similar assessment can determine the effect of strengthening the afore-mentioned areas. Thus, the Test Bed demonstration has shown the directed graph-fault tree procedure (Figure 3) to be an effective assessment tool. The procedure can also be used for safety and reliability analysis.

3.2 Storage Tank Example

An application of the directed graph-fault tree methodology is illustrated by an example in the Appendix. The example consists of a storge tank of plutonium nitrate with a differential pressure cell used to measure the solution mass. The tank is located in a protected area called a material access area, MAA. The MAA is

protected by a roving guard and a guard stationed outside the MAA.

4. CURRENT ACTIVITIES

Alternative and complementary material control assessment procedures have been developed and tested at Lawrence Livermore Laboratory.

One alternative approach is the Logic Diagram Model as described by Lim and Huebel.[11] The logic diagram models the information flow in a way similar to that of the digraph. The logic diagram is a Boolean logic model and Boolean equations are defined directly on the logic model. On the other hand, the digraph is a multi-valued logic model and a synthesis algorithm is needed to generate a fault tree. Both approaches have advantages and disadvantages. The digraph-fault tree approach is more complex to use. It requires that the loops in the system digraph be found and a synthesis algorithm be used. The logic model approach is simpler to generate, however, the logic model contains in general many Inhibit gates which generate NOT gates and efficient prime implicant algorithms must be used.[12,13] Current computer codes do not easily handle a large number of equations with complemented events.

Another approach, the Structured Assessment Approach, models the movement of SNM and the flow of information in the material control system by adjacency matrices. One output of the approach are target sets, the sets of conditions and monitor failures that permit successful theft of SNM to occur. The approach is described in detail by Sacks et al.[14]

APPENDIX A: EXAMPLE OF THE USE OF THE DIGRAPH-FAULT TREE METHODOLOGY

The objective of the digraph-fault tree methodology is to systematically produce a fault tree for qualitative and quantitative evaluation. A fault tree is deductive Boolean logic model of a Top Event, an undesired event or system state.

The Top Events are events such as "fire", "explosion", or "system shutdown" for safety and reliability analyses. For material control assessment, the Top Event can be an event such as "Successful theft of SNM from the facility." The Top Event is defined in terms of basic events which provide the limit of resolution for the fault tree.

The basic events in safety and reliability analysis include human error, equipment failure, and environmental conditions. For material control assessment, the basic events include adversary activity, such as equipment destruction and records falsification, in addition to those given above.

A brief description of the digraph-fault tree terminology and notation is now presented.

A.1 NOTATION AND TERMINOLOGY

A digraph is a set of nodes and connecting edges. Nodes in the digraph represent events. If one variable effects another variable or event, a directed arrow or edge connects the independent variable to the dependent one. The directed edge may either be a normal edge which indicates the relationship is normally true, or a conditional edge which indicates the relationship is true only when another event (or condition) exists. Edges connecting any pair of nodes are mutually exclusive; only one edge relationship is true at a given time.

Numbers may be placed on the directed edge to represent the gains between the two events. These gains are based on the mathematical definition of gain, $\partial Y/\partial X$, where X and Y denote the independent and dependent variables or events respectively. The magnitudes of the gains used in the digraphs for the assessment are quantized into three discrete values of -1, 0, +1. Gains of ± 1 represent normal disturbances which a negative feedback loop is able to cancel. Gains of 0 indicate the nullification of any relationship existing between the two events.

Events are represented by alphanumeric labels on the nodes. For instance "P2", M3", FIRE at HX" represent pressure at location 2, mass flow rate at location 3, and fire at heat exchanger, respectively. The direction of the deviations in the values of variables are

denoted by "+" and "-". These deviations have magnitudes of "0" and "1". Magnitude of 1 indicates a range of values that is considered moderate. A magnitude of 0 represents a true or expected range of values of the event. The same scheme of -1, 0, +1, is also used to represent the deviations in the values of events. For instance P2(0) represents the true or expected value of pressure at location two, and M3(+1) represents a moderate mass flow rate at location 3.

Some events may be univariant; that is, they deviate only in the positive direction or only in the negative direction. For instance, "FIRE at HX" is a univariant variable.

A.2 UNIT MODEL DIGRAPHS

An example to illustrate unit model digraph generation is now given.

Fig. A.1 shows a storage tank containing plutonium nitrate with a differential pressure cell. The solution mass in the tank is determined by measurement of the difference between pressures P_1 and P_2 given by the following relationship:

$$\text{STATIC PRESSURE} = \rho g(L-L_1) = p_1-p_2$$

where ρ is the solution density, g is the acceleration constant due to gravity, L is the level of solution in the tank and L_1 is the level at which air enters the tank at line 1. An air supply (not shown) provides air to lines 1 and 2.

The glove box shown in Fig. A.1 is used to sample plutonium nitrate from the storage tank via the sample line. A technician transfers the sample through a pneumatic sample line to the laboratory for chemical analysis.

In order to safeguard the plutonium nitrate solution, the material control system will notify security when the following stimuli are received:

- Loss of vacuum detected by a pressure sensor on the glove box
- Change in solution mass determined by a differential pressure cell measurement

Then MC procedure requires a security guard to be sent to the MAA entrance in the event an anomolous signal is received and apprehend anyone stealing SNM. Also, a roving guard is required to inspect the glove box and apprehend anyone stealing SNM.

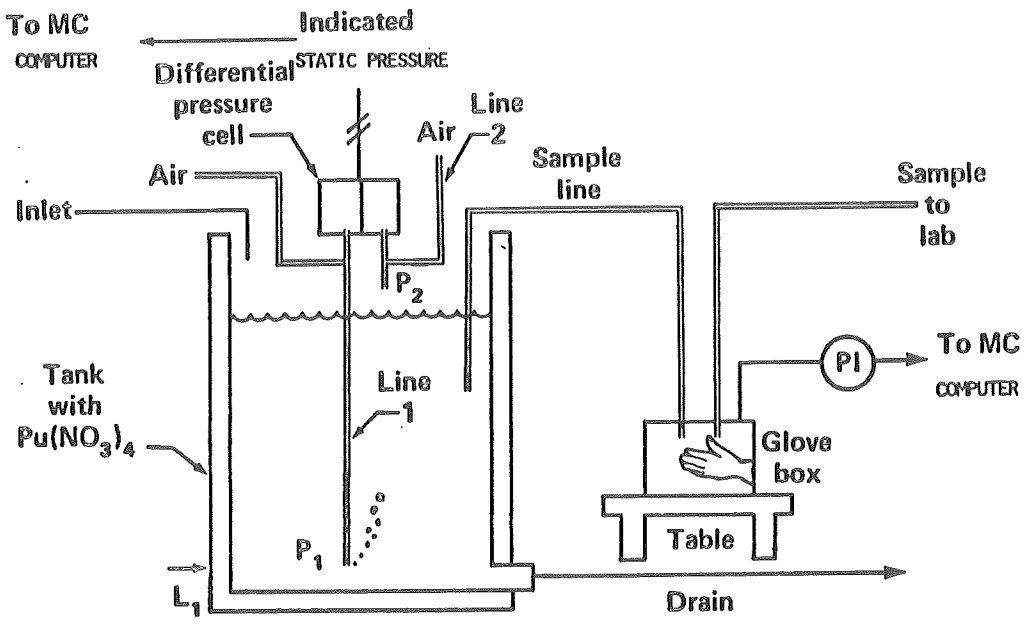

Fig. A.1. Storage Tank with Differential Pressure Cell

Figures A.2, A.3, A.4 and A.5 show respectively unit model digraphs of the following:

- Glove box with pressure sensor
- Storage tank with differential pressure cell
- MC computer decision logic
- Roving guard

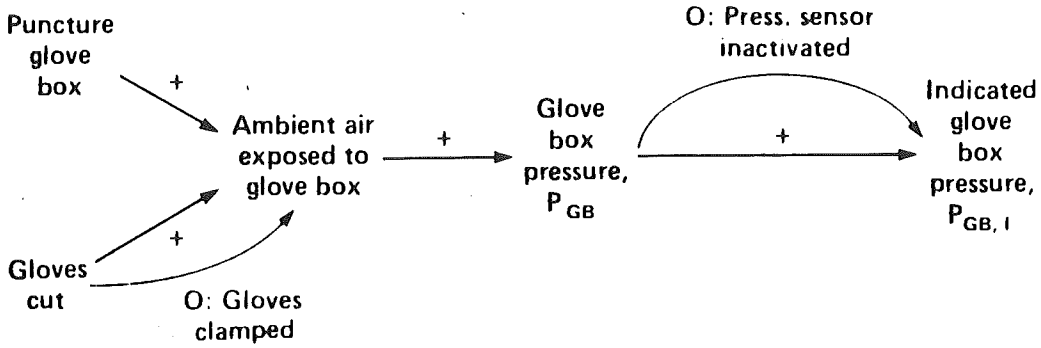

Fig. A.2. Unit Model Digraph of Glove Box with Pressure Sensor

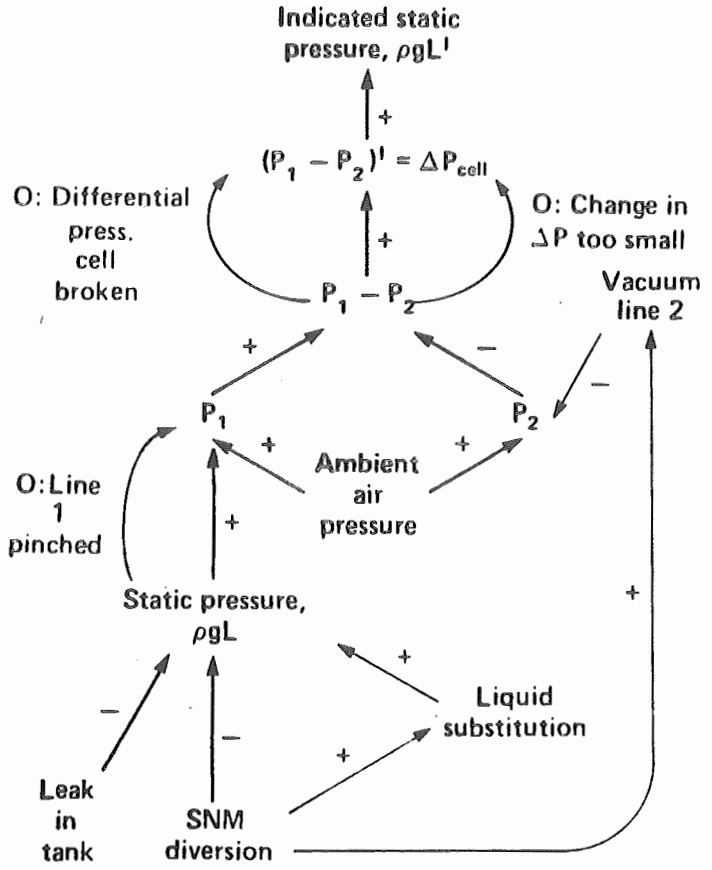

Fig. A.3. Unit Model Digraph of Storage Tank with Differential Pressure Cell

By definition successful theft of SNM occurs when SNM crosses the boundary ot the MAA. For this to occur, the adversary must perform a minimum necessary and sufficient set of acts to get SNM out of the MAA. These acts include:

- Movement within MAA
- Penetration of the glove box
- Removal of SNM from sampler

As the result of attempting these acts, signals will be generated and an MC response generated. If successful theft is to occur, the information flow associated with these signals must be nullified. As shown in the unit model digraphs, there are two ways that the information flow can be nullified:

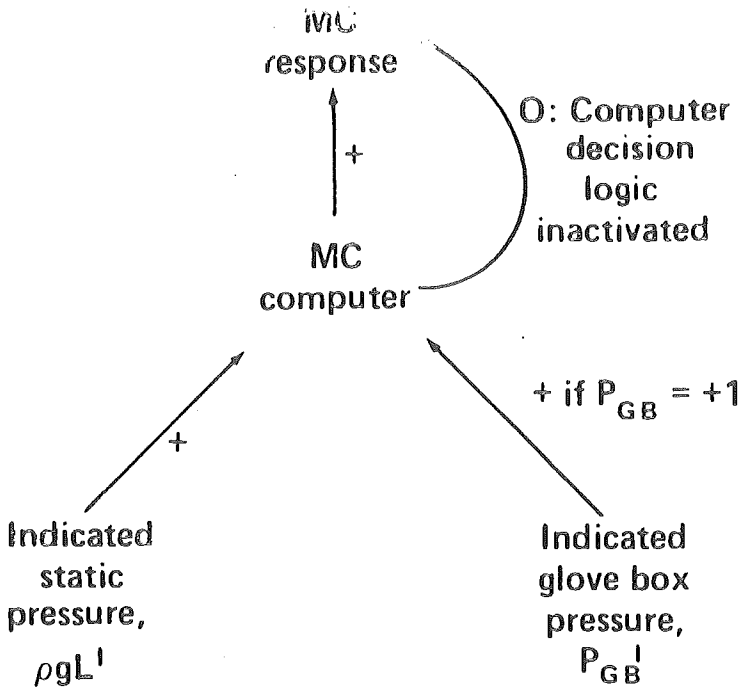

Fig. A.4. Unit Model Digraph of MC Computer Decision Logic

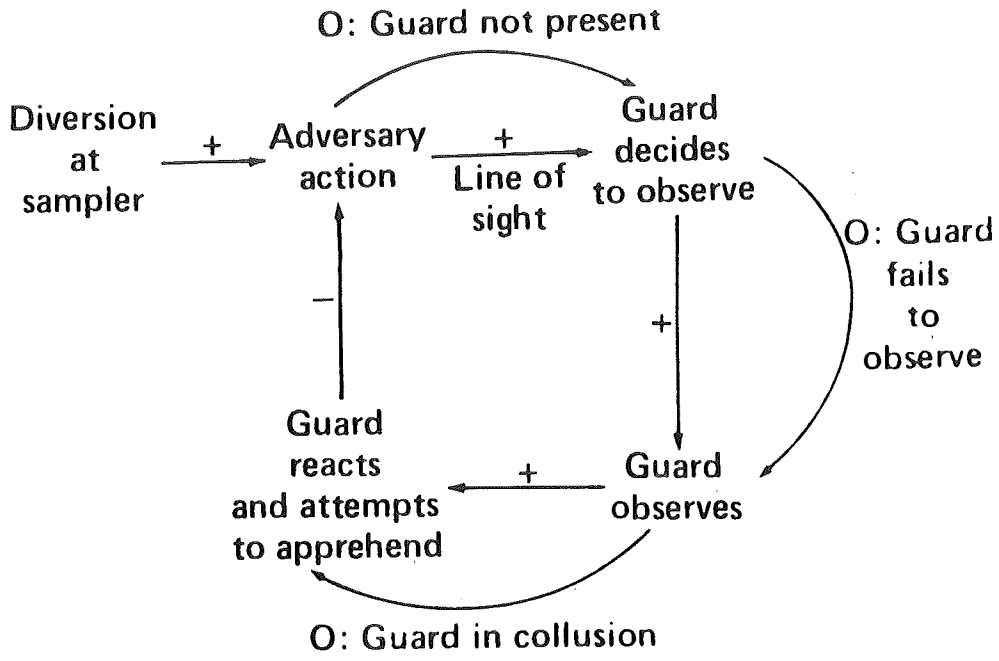

Fig. A.5. Unit Model Digraph of Roving Guard

- Zero gain events (events following the zero on the edges of the digraphs) that cause an MC component to be inactive such as human, equipment failure and measurement insensitivy
- Stimulus variable cancellation resulting in no signal when an adversary activity is committed. Stimulus refers to a disturbance in an MC variable that occurs as the result of adversary activity. As an example, refer to Fig. A.3. If an adversary steals SNM at the glove box and simultaneously adds liquid to the tank or applies a vacuum on line 2, then the indicated solution mass will not change and a signal will not be generated

A.3 SYSTEM DIGRAPH GENERATION

The unit model digraphs described previously are linked together to form the system digraph by starting at the node, $M_{DIV,MAA}$ defined by:

$$M_{DIV,MAA} = \begin{cases} +1 \text{ successful theft of SNM from the MAA} \\ 0 \text{ otherwise} \end{cases}$$

Digraphs are generated in a similar manner as fault trees are constructed. One starts from the Top Event variable, works strictly backwards (i.e., deductively) and determines variables that can directly cause a disturbance in the variable under development. This causal information is obtained from either the unit model digraph or from the connectivity information in the system schematic. The limit of resolution is reached when variables are encountered which have no inputs. These variables are called primal variables (similar in scope to basic events in fault trees).

Using the process described above, we generate the system digraph as shown in Fig. A.6. The corrective actions of the material control system are modeled as negative feedforward loops (NFFL's) and negative feedback loops (NFBL's).

A NFFL consists of two or more paths which start at the same node and merge together at a different node. NFFL's have the property that the sign of the normal gains on one path (i.e., without failures) is different from the other paths. In contrast, a NFBL is path which starts and ends at the same node. NFBL's have the property that the product of the normal gains around the NFBL is negative.

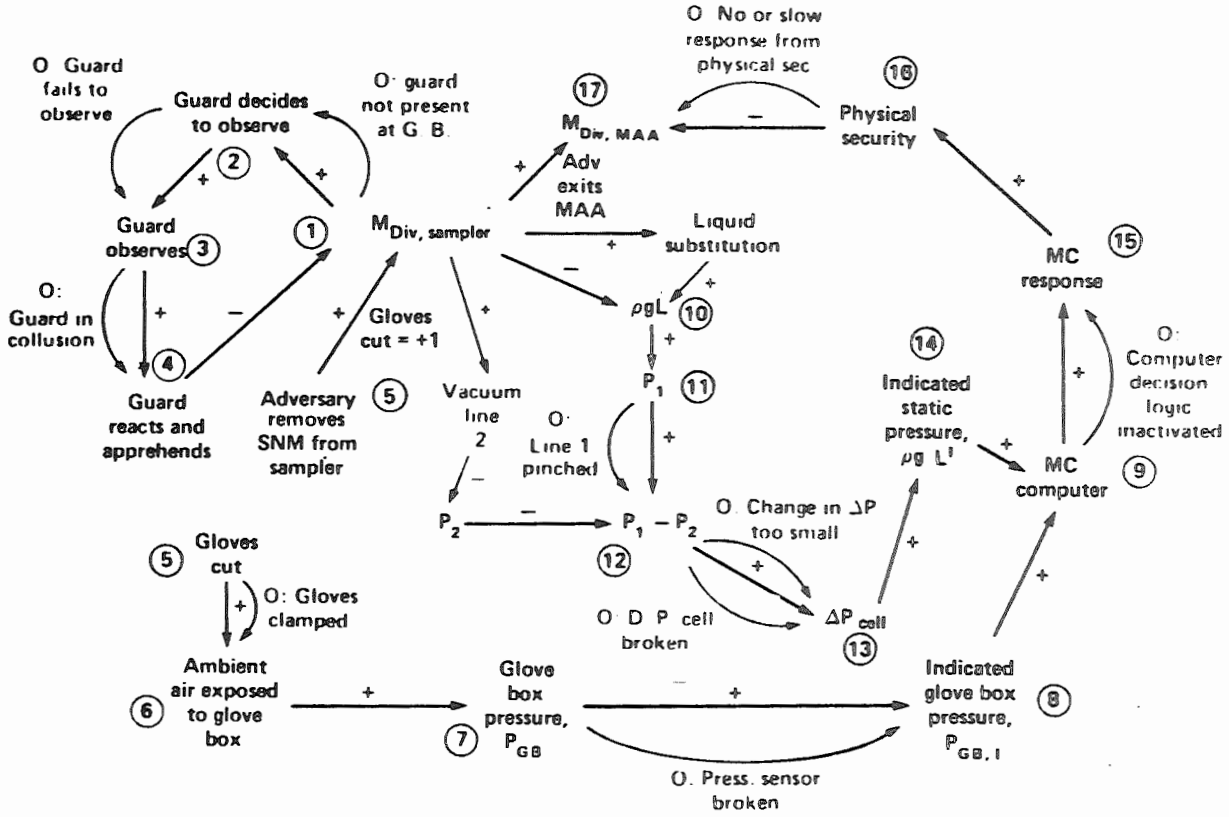

Fig. A.6. System Digraph

There is one NFBL in the system digraph in Fig. A.6

- Response from roving guard (nodes 1,2,3 and 4)

and two NFFL's

- Response from security to change in static pressure
  path 1 - (nodes 1 and 17)
  path 2 - (nodes 1,10,11,12,13,14,9,15,16 and 17)
- Response from security to change in golve box pressure
  path 1 - (nodes 5,1 and 17)
  path 2 - (nodes 5,6,7,8,9,15,16 and 17)

Path 1 for the two NFFL's describes the conditions necessary for SNM movement out of the MAA. Path 2 represents the corrective action of the MC system in preventing SNM theft.

A.4 FAULT TREE GENERATION

The fault tree is constructed from the system digraph via a synthesis algorithm, [9,14] starting from the top event node, $M_{DIV,MAA}$. For MC assessment, the algorithm generates AND gates in two basic ways:

- The adversary attempts to steal SNM and conditions must be satisfied for removal of SNM
- The adversary commits an act which generates a signal and the MC system fails to respond to the signal because the corrective action of the NFBL or NFFL fails

The fault tree constructed using the synthesis algorithm is shown in Fig. A.7. Examination of the fault tree shows that all three loops must fail for successful theft to occur.

A.5 QUALITATIVE ANALYSIS

The minimal cut sets of the fault tree in Fig. A.7 are the adversary event sets. There are 36 event sets as shown in factored form in Fig. A.8: 33 event sets generate no MC response and three event sets generate an inadequate response.

The first line in Fig. A.8 represents the conditions necessary for removal of SNM, (See system digraph in Fig. A.6.). The second line in Fig. A.8 represents the basic events necessary to fail the roving guard, i.e., the NFBL. The third line represents the "common mode" events that can simultaneously fail both NFFL's. The

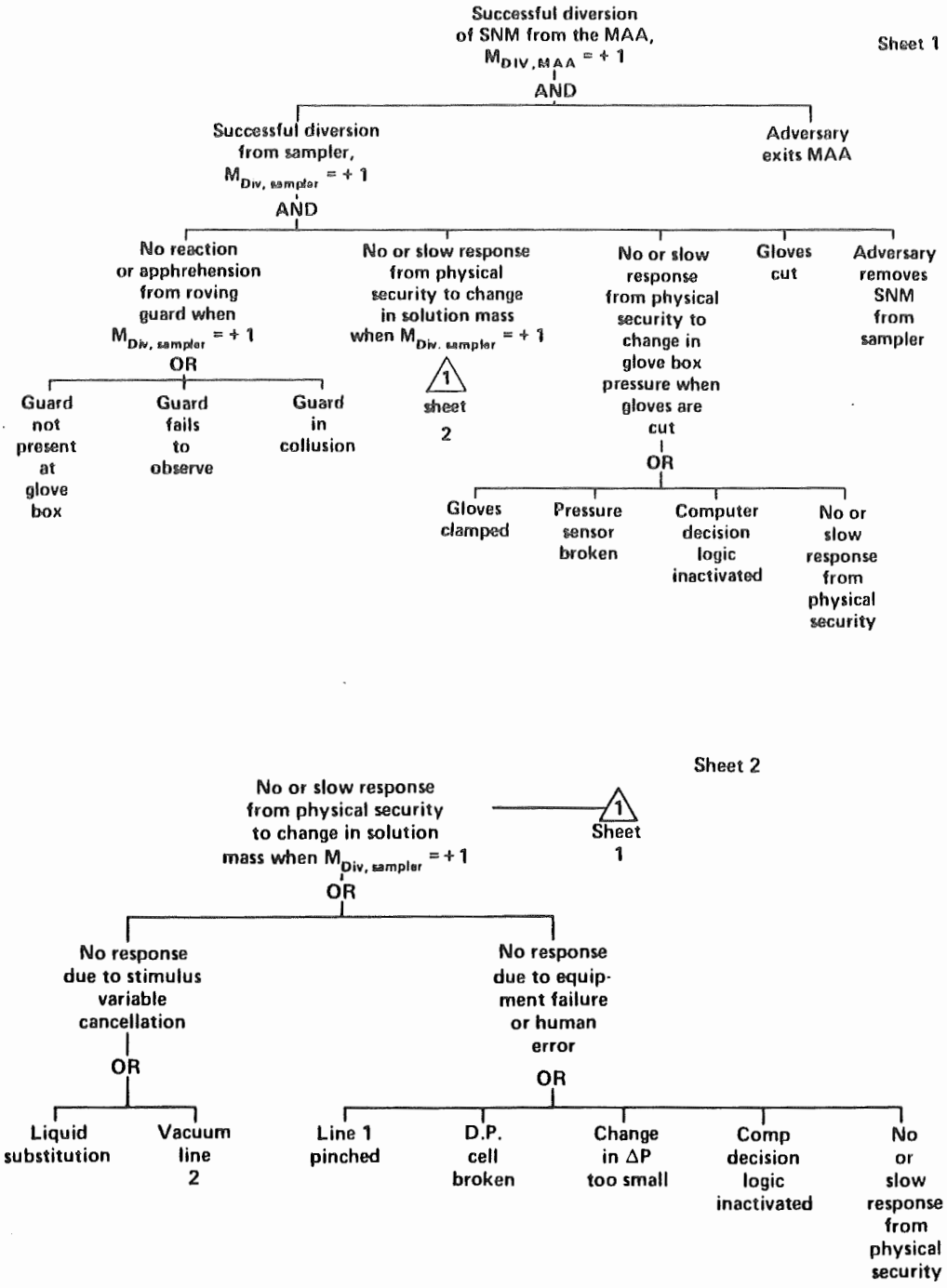

Fig. A.7. Fault Tree for Successful Diversion from Storage Tank

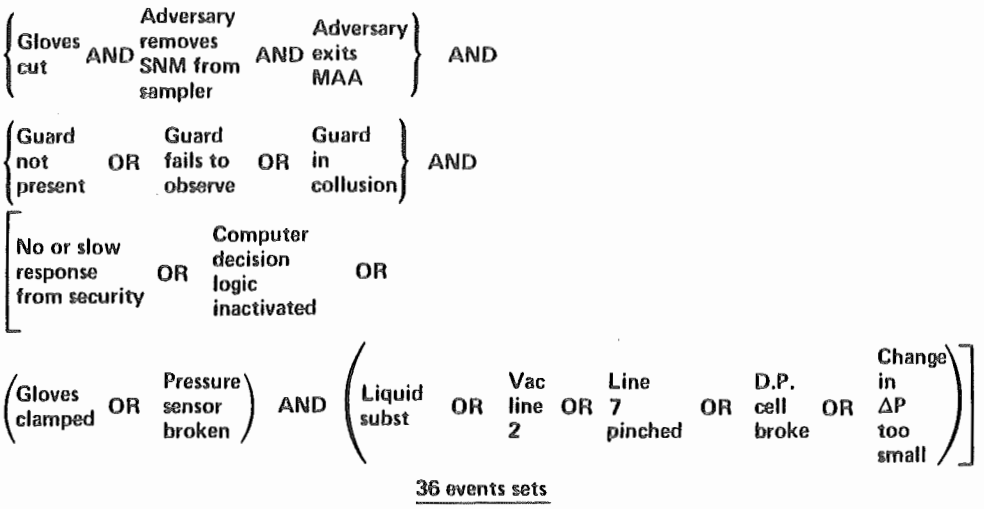

Fig. A.8. Event Set Representation in Factored Form

fourth line represents 10 combinations of basic events taken two-at-a-time that fail both NFFL's.

By performing a Boolean substitution for the basic events in terms of plant personnel who can perform the events, the collusion requirements for the event sets are determined:

- 22 event sets can be accomplished solely by the technician or the roving guard
- 11 event sets can be accomplished by two people -- the technician and the roving guard in collusion
- 3 event sets can be accomplished by three people -- the technician, the roving guard and the guard at the security station in collusion

Much useful information can be obtained without quantitative information. We see the usefulness of the system digraph in displaying system topology and information flow.

A.6 OTHER CONSIDERATIONS

The authors[9] and Sacks et al.[14] discuss in detail the reliability assessments of MC systems. The assessments must consider tampering, records falsification and equipment destruction. The importance of a reliability analysis is not so much the absolute numbers that result but the sensitivity analysis which indicates

the relative strengths and weaknesses of the MC system in quantitative terms.

The example in this appendix did not discuss the incorporation of consistency check in the fault tree analysis. Consistency checks are important in considering the interaction of time periods, i.e., an adversary can take advantage of monitors that are inactive during various modes of operation. In addition, the example did not consider the incorporation of dynamics in the analysis, i.e., given that anomolous signals are generated, is the MC response fast enough? These matters are considered in detail by the authors.[9]

REFERENCES

1. A. Maimoni, "Safeguards Research: Assessing Material Control and Accounting System," Energy and Technology Review, Lawrence Livermore Laboratory, Rept. UCRL-52000-77-11/12 (1977).*
2. S. A. Lapp and G. J. Powers, "Computer Aided Synthesis of Fault Trees" in IEEE Trans on Rel. R-26 (1)(1977).
3. H. E. Lambert and J. J. Lim, The Modeling of Adversary Action for Safeguards Effectiveness Assessment, Lawrence Livermore Laboratory, Rept. UCRL-79217, Rev. 1 (1977).*
4. J. B. Fussell et al., A Collection of Methods for Reliability and Safety Engineering, Idaho National Engineering Laboratory, Idaho Falls, Rept. ANCR-1273 (1976).*
5. S. L. Salem, G. E. Apostolakis, and D. Okrent, "A New Methodology for the Computer-Aided Construction of Fault Trees," Annals of Nuclear Energy, 4 (1977) 417-433.
6. R. Willie, Fault Tree Analysis Program, Operations Research Center Report No. ORC 78-14, University of California, Berkeley (1978); Rept. UCRL-13981, Lawrence Livermore Laboratory.*
7. R. B. Worrell, Set Equation Transforation System (SETS), Sandia Laboratories, Albuquerque, New Mexico, Rept. SLA-73-0028A (1974).*
8. H. E. Lambert and F. M. Gilman, The IMPORTANCE Computer Code, Lawrence Livermore Laboratory, Rept. UCRL-79269 (1977).*
9. H. E. Lambert, J. J. Lim and F. M. Gilman, A Digraph-Fault Tree Methodology for the Assessment of Material Control Systems, Lawrence Livermore Laboratory, Rept. UCRL-52170 (1979).*
10. I. J. Sacks, et al., Material Control System Design: Test Bed Nitrate Storage Area (TBNSA), Lawrence Livermore Laboratory, Rept. UCID-17525-77-3 (1978).*
11. J. J. Lim and J. G. Huebel, Modeling Adversary Actions Against a Nuclear Material Accounting System, Proceedings of the 1st annual ESARDA Symposium on Safeguards and Nuclear Material Management, Palais des Congres, Brussels (1979).

12. B. L. Hulme and R. B. Worrell, "A Prime Implicant Algorithm with Factoring," IEEE Trans. on Computers, (November, 1979).
13. R. R. Willie, Computer Oriented Methods for Assessing Complex System Reliability, Ph.D. Thesis, Dept. of Operations Research, U.C. Berkeley, (1979).
14. I. J. Sacks, A. A. Parziale, T. R. Rice, S. L. Derby, The Structured Assessment Analysis of Facility X, Volume 1 - Executive Summary, MC 79-12-D, Lawrence L vermore Laboratory, to be published as a NUREG Report (1979).*

---

* Available from National Technical Information Service, Springfield, VA 22151, USA.

12. B. L. Hulme and R. B. Worrell, "A Prime Implicant Algorithm with Factoring," IEEE Trans. on Computers, (November, 1979).
13. R. R. Willie, Computer Oriented Methods for Assessing Complex System Reliability, Ph.D. Thesis, Dept. of Operations Research, U.C. Berkeley, (1979).
14. I. J. Sacks, A. A. Parziale, T. R. Rice, S. L. Derby, The Structured Assessment Analysis of Facility X, Volume 1 - Executive Summary, MC 79-12-D, Lawrence L vermore Laboratory, to be published as a NUREG Report (1979).*

---

* Available from National Technical Information Service, Springfield, VA 22151, USA.